AFFIDAVIT
OF
JOSHUA B. COOPER
FEDERAL BUREAU OF INVESTIGATION

I, Joshua B. Cooper, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Kansas City Division, Jefferson City Resident Agency in Jefferson City, Missouri. As such, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included each and every fact known to me concerning this investigation. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described below. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(l)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I below, Upon receipt of the information described in Section I, government-authorized persons will review that information to locate the items described in Section II.

Property to Be Searched

3. This warrant applies to information associated with scufingenenf3@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheater Parkway, Mountain View, California.

4. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, malicious software, the theft of personal identification information, and other computer-based fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received training in computer technology and computer-based fraud.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030 and 1343 have been committed by unknown persons. There is also probable cause to search the information described above for evidence, instrumentalities, and/or fruits of these crimes.

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described above is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed above:

a. The contents of all emails associated with the account January 1, 2022 to December 31, 2023, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 30 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1030 and 1343, those violations involving scufingenenf3@gmail.com, including, for each account or identifier listed above, information pertaining to the following matters:

a. Preparatory steps taken in furtherance of the fraud scheme;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

4. As a Special Agent with the FBI, I investigate criminal and national security related computer intrusion matters involving botnets, malicious software, the theft of personal identification information, and other computer-based fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received training in computer technology and computer-based fraud.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030 and 1343 have been committed

by unknown persons. There is also probable cause to search the information described above for evidence, instrumentalities, and/or fruits of these crimes.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711; 18 U.S.C. §§ 2703(a), (b)(l)(A), & (c)(l)(A). Specifically, the Court is "a district court of the United States ... that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711 (3)(A)(i).

PROBABLE CAUSE

8. On October 26, 2023 B.M. logged into his/her Trezor hardware wallet from his/her home office to confirm that a transfer s/he recently made into the wallet had arrived as well as to send one Ethereum (ETH) token to another exchange account. When B.M. logged in to his/her wallet, s/he successfully confirmed the transfer had arrived and proceeded to transfer the one ETH out of his/her account as intended.

9. B.M. then noticed a couple of offers that existed in his/her Trezor wallet claiming that s/he had accrued rewards in his/her wallet that could be claimed at a few various websites. Airdrops and rewards are a relatively standard occurrence in the crypto currency industry.

10. B.M. proceeded to a website from one of the offers which claimed to have $7,600 USD available to claim. This website was usd-coin.org. When B.M. pulled up the website it had the appearance of being an official website sponsored by Circle, the creator of the stablecoin USDC. There was a prompt for B.M. to connect his/her wallet in order to complete the transfer of the rewards tokens. When B.M. clicked “connect my wallet” s/he was prompted to enter the twelve word seed phrase in conjunction with his/her Trezor wallet. B.M. believed it was his/her Trezor device asking for the seed phrase when in fact it was the malicious website. B.M. entered his/her

twelve word seed phrase as prompted and got another prompt that the seed phrase was invalid. B.M. became leery at this point and did not further pursue the bonus funds.

11. Thereafter, B.M. noticed the first of many unauthorized transfers from his/her device. Over the next 24 minutes numerous transfers occurred without approval or prompting from B.M. resulting in a total loss of approximately $533,993.71 which was the asset value at the moment of the theft.

12. The user email associated with the malicious website usd-coin.org is scufingenenf3@gmail.com. The account is active and the user IP is 185.220.103.6. The site is hosted at IP 13.227.219.64. On approximately July 14, 2010, an unknown individual, using the name Eugena Martinez, registered the domain usd-coin.org. This individual subsequently used this domain to defraud B.M. of cryptocurrency.

BACKGROUND CONCERNING EMAIL

13. In my training and experience, I have learned that Google LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google LLC allows subscribers to obtain email accounts at the domain name @gmail.com, like the email account scufingenenf3@gmail.com. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. A Google LLC subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

15. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

16. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the

account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

17. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

18. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the

physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

19. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING AND NON-DISCLOSURE ORDER

20. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

21. There is reason to believe that notification of the existence of this Application and any Court order issued will seriously jeopardize the investigation, including giving the subjects. an opportunity to: flee, destroy or tamper with evidence; change his or her pattern of behavior, or notify any confederates. See 18 U.S.C. § 2705(b)(2),(3),(5). As such, the United States further requests, pursuant to 18 U.S.C. §§ 3123(d)(2) and 2705(b), that the Court order Google, Inc. and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, or this investigation, except as necessary to effectuate the Order, for one year from the date of this Order unless otherwise ordered by this Court. I request these documents may be disclosed as required for discovery purposes without further order of this Court.

22. The facts set forth in this affidavit are true and correct to the best of my knowledge and belief.

Joshua B. Cooper
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, on this, the 6th day of March 2024.

Willie J. Epps, Jr.
Chief United States Magistrate Judge